



# *Information Security*

**National Workshop on Biosecurity  
Thailand Science Park, Pathumthani, Thailand  
27–28 September, 2004**

**Natalie Barnett  
Sandia National Laboratories**



# Information Security

- **What is information security?**
  - To restrict access to information that is determined by the institution to be too sensitive for general distribution.
- **What information is at risk?**
  - Information that may be considered too sensitive for general distribution includes, but is not limited to, information related to personnel, financial records, or the security of dangerous pathogens and toxins.



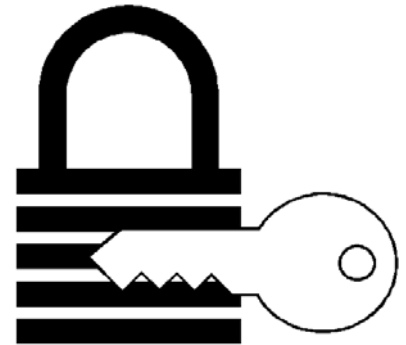
# Sensitive Information

- **Sensitivity levels**

- Low (open or public information)
- Moderate (limited access information)
- High (exclusive or strict access information)

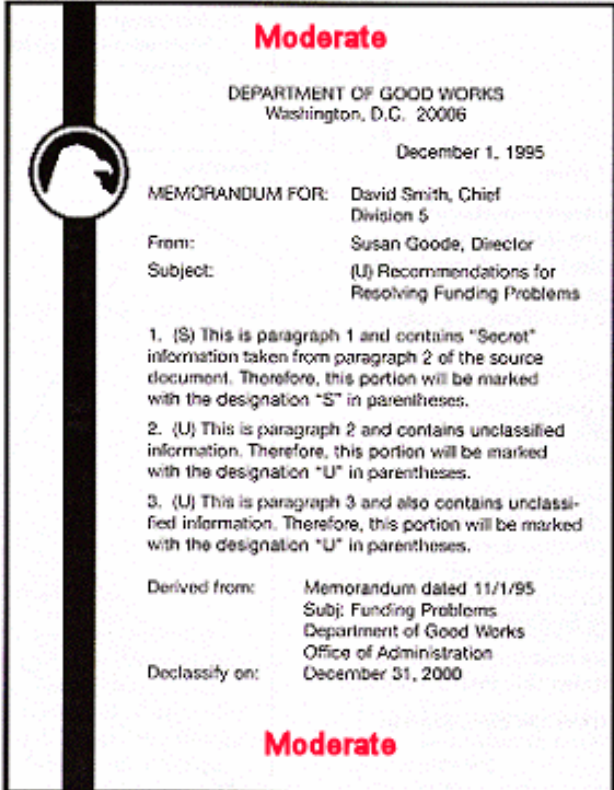
- **Some examples of information assets:**

- Personnel information
- Facility details
  - ◆ Physical security information
  - ◆ Network security information
- Specific information on pathogens and toxins
  - ◆ Databases
  - ◆ Lab records
- Security procedures
- Scientific papers



# Marking

- Moderately and highly sensitive information should be labeled
  - Sensitivity level designation
  - Top and bottom of each page / cover sheet
- Marking and control methods should be well understood by those working with information



**Moderate**

DEPARTMENT OF GOOD WORKS  
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief  
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for  
Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

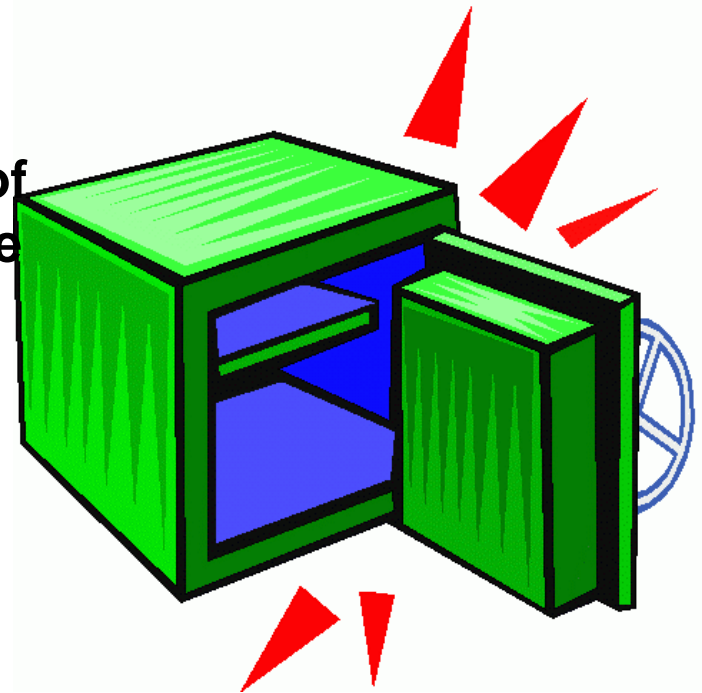
Derived from: Memorandum dated 11/1/95  
Subj: Funding Problems  
Department of Good Works  
Office of Administration

Declassify on: December 31, 2000

**Moderate**

# Control

- The control of moderate and high risk information should be the direct responsibility of the individual with the information
- This includes the physical security of the information and places where the information is stored

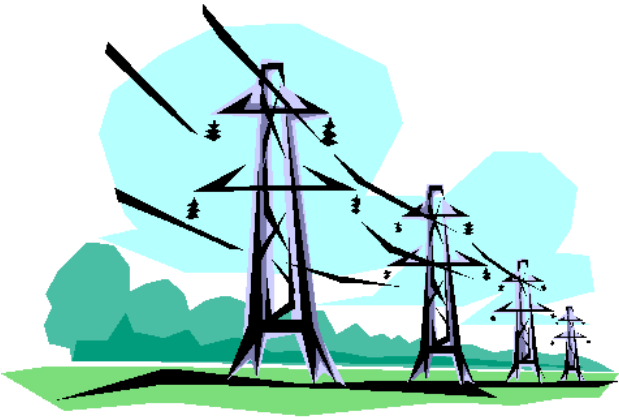




# Communication

---

- **Insecure transmission of information can lead to accidental release**
- **Transmission of moderately or highly sensitive information should only occur via approved methods**
  - **Mail, email, or fax security is required**
  - **Limited discussions in open areas**
  - **Information should only be reproduced when needed and each copy must be controlled as the original**



# Network Security



- **Network Management**

- **The network on which all information is transmitted should be protected**
  - ◆ Infrastructure
  - ◆ Servers
  - ◆ Remote access
  - ◆ Wireless

- **Users**

- **Each system within the network should maintain a level of security**
  - ◆ Network layered access
  - ◆ Desktop security
  - ◆ Wireless

# Policies



- **Realistic policies**
  - Policies should be comprehensive
  - Policies should allow for users to work as needed
- **Understanding of policies by all users**
  - Having clear policies is critical to users following them
  - The policies should be easy to locate, understand, and follow





# Summary

---

- **Information security is critical to biosecurity**
- **Information at risk may include:**
  - Personnel information
  - Physical security information
  - Specific information on pathogens and toxins
- **Information security is comprised of understanding:**
  - Levels of sensitivity
  - Risks to information
  - Information policies
  - Practice